Mitigating IT Risk at the Enterprise Level with Actionable Governance

71% of business leaders now believe that their success or failure will be defined by technology. IT oversight and governance can no longer be limited to a single department, but must be propagated throughout business lines and ultimately to senior management and the board.

- 78% of paid Android and iOS apps have hacked variants in the wild[1]
- 6 of 10 employees ages 18-35 use a personal device for work[1]
- 3.6M ZeuS botnet infected computers were detected in the U.S. In 2009[2]
- 30M new malware strains circulated in 2013[2]
- 156M phishing emails per day in the US with a click ratio of 0.5% (do the math for your business)[3]
- 33% of exploited vulnerabilities were from Web Applications[4]

Define, collect and monitor metrics.

Identify

Define the environment, understand the context.

Risk identification is an iterative process. New risks will be identified as the project progresses through the life cycle.

Establishing a clear framework of goals and objectives, empowers the business to easily recognize, prioritize and classify risk effectively and appropriately.

This framework facilitates a consistent classification of assets through confidentiality, integrity and availability (CIA) requirements, providing a clear picture of the environment and driving the requirement levels and prioritization of subsequent remediations.

Track

Monitor and control.

The development of risk management performance metrics is essential to risk monitoring success - and to driving performance across the business.

The establishment of a management indicator system that provides accurate, timely, and relevant risk information in a clear, easily understood manner is key to risk monitoring. Early in the planning phase of the process, the team should identify specific indicators to be monitored and information to be collected, compiled, and reported.

Assess

Investigate, analyze, understand and prioritize.

Determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat enables the organization to understand the business context of their overall vulnerabilities - and prepare for and mitigate loss.

Continuous self-assessment and continuous controls monitoring creates a clear line of accountability, reduces the risk of fraud (by examining data that may flag unusual patterns of transactions) and results in an organization with a lower risk profile.

Manage

Accept | Avoid | Transfer | Mitigate

Risk mitigation involves prioritization, evaluation and implementation of appropriate risk reducing activities as a result of the risk assessment process. Leadership must balance the cost and effectiveness of the proposed risk-reducing activities against the risk being addressed.

Enterprise mitigation strategies must be commensurate with risks identified by risk assessments. For those risks where the mitigation strategy involves the use of controls, those controls must ensure that risks are reduced to an acceptable level, taking into account:

- Legal and regulatory requirements and compliance.
- Enterprise operation and policy requirements and constraints.
- Cost of implementation, maintenance, and operation.

Chief Risk Officer (CRO)

IT Risk Governance

Finding the right balance between opportunity, risk and control is a continuous cycle that organizations must consistently adapt and refine to stay agile in an uncertain and evolving business climate.

Monitor and verify mitigation plan progress.

IBM enables organizations to combine deep understanding of IT threats and vulnerabilities with insight into how these might affect business performance, enabling you to build a sustainable risk and compliance approach that aligns IT with corporate initiatives, strategy and regulatory requirements.

Find out more ibm.biz/ITG_Video

Sources:

[1] Arxan, an IBM Business Partner
[2] http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report_2013.pdf
[3] http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx
[4] XForce report, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGL03045USEN&attachment=WGL03045USEN.PDF

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2014

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.